(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号
特開2000－231760
（P2000－231760A）
(43)公開日　平成12年８月22日(2000.8.22)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ	20/10	Ｈ
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ	1/00	６６０Ｄ
Ｇ１１Ｂ　19/04	５０１	Ｇ１１Ｂ	19/04	５０１Ｈ
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ	9/00	６０１Ａ

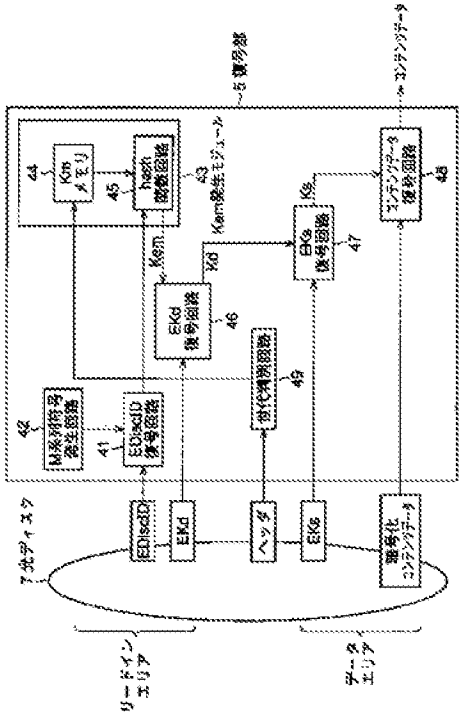
審査請求　未請求　請求項の数23　ＯＬ　（全 12 頁）

(21)出願番号　特願平11－344396
(22)出願日　平成11年12月３日(1998.12.3)
(31)優先権主張番号　特願平10－352975
(32)優先日　平成10年12月11日(1998.12.11)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　浅野　智之
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　大隈　義知
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100082131
弁理士　稲本　義雄

(54)【発明の名称】　情報記録装置および方法、情報再生装置および方法、並びに記録媒体

(57)【要約】
【課題】　秘密キーを更新した場合でも、古い世代の秘密キーを用いて暗号化データを復号できるようにする。
【解決手段】　光ディスク７には、暗号化コンテンツデータを暗号化したセクタキーEksの世代が書き込まれている。世代判別回路４９は、暗号化に用いられたセクタキーEksの世代を判別する。Kmメモリ４４は、判別された世代に対応したマスタキーKmをEkd復号回路４６に出力する。Ekd復号回路４６は、暗号化されたディスクキーEkdを、マスタキーKmを用いて復号する。Ekd復号回路４７は、ディスクキーKdを用いて、暗号化されたセクタキーEksを復号し、セクタキーksを得る。コンテンツデータ復号回路４８はセクタキーKsを用いて、暗号化コンテンツデータを復号する。



【特許請求の範囲】
【請求項１】　着脱可能な記録媒体にデータを記録する情報記録装置において、
少なくとも１以上の世代の秘密鍵を記憶する記憶手段と、
前記記録媒体の媒体識別情報と前記秘密鍵から第１の鍵を生成する生成手段と、
前記記録媒体に記録する前記データを暗号化するために用いる第２の鍵を前記第１の鍵で暗号化する第１の暗号化手段と、
前記第１の暗号化手段により暗号化された前記第２の鍵を、前記第１の鍵の世代番号とともに前記記録媒体に記録する第１の記録手段とを備えることを特徴とする情報記録装置。
【請求項２】　前記媒体識別情報を、乱数として発生させる第１の乱数発生手段をさらに備え、
前記第１の暗号化手段は、前記記録媒体が予め前記第２の鍵を有している場合、前記記録媒体から前記第２の鍵を読み出し、前記記録媒体が前記第２の鍵を有していない場合、前記第１の乱数発生手段に前記第２の鍵となる乱数を発生させることを特徴とする請求項１に記載の情報記録装置。
【請求項３】　前記記録媒体は、複数の記録単位に分割されており、
前記記録単位に記録する前記データを暗号化する第３の鍵となる乱数を前記記録単位毎に発生させる第２の乱数発生手段と、
前記第２の乱数発生手段により発生された前記第３の鍵を、前記第２の鍵で暗号化する第２の暗号化手段と、
前記第２の暗号化手段により暗号化された前記第３の鍵を前記記録媒体の記録単位に記録する第２の記録手段とをさらに備えることを特徴とする請求項２に記載の情報記録装置。
【請求項４】　前記第２の鍵は、前記記録媒体毎に固有の値とされるとともに、前記秘密鍵の世代が変わる毎に、前記第１の乱数発生手段により新規に生成されることを特徴とする請求項２に記載の情報記録装置。
【請求項５】　前記記憶手段は、１世代の前記秘密鍵を記憶し、演算により他の世代の前記秘密鍵を生成することを特徴とする請求項１に記載の情報記録装置。
【請求項６】　前記第１の鍵の世代番号は、前記生成手段で用いた前記秘密鍵の世代に対応することを特徴とする請求項１に記載の情報記録装置。
【請求項７】　着脱可能な記録媒体にデータを記録する情報記録装置の情報記録方法において、
少なくとも１以上の世代の秘密鍵を記憶するように記憶を制御する記憶制御ステップと、
前記記録媒体の媒体識別情報と前記秘密鍵から第１の鍵を生成する生成ステップと、
前記記録媒体に記録するデータを暗号化するために用いる第２の鍵を前記第１の鍵で暗号化する第１の暗号化ステップと、
前記第１の暗号化ステップの処理により暗号化された前記第２の鍵を、前記第１の鍵の世代番号とともに前記記録媒体に記録するように記録を制御する第１の記録制御ステップとを含むことを特徴とする情報記録方法。
【請求項８】　前記媒体識別情報を、乱数として発生させる第１の乱数発生ステップをさらに含み、
前記第１の暗号化ステップの処理では、前記記録媒体が予め前記第２の鍵を有している場合、前記記録媒体から前記第２の鍵を読み出し、前記記録媒体が前記第２の鍵を有していない場合、前記第１の乱数発生ステップの処理により前記第２の鍵となる乱数を発生させることを特徴とする請求項７に記載の情報記録方法。
【請求項９】　前記記録媒体は、複数の記録単位に分割されており、
前記記録単位に記録する前記データを暗号化する第３の鍵となる乱数を前記記録単位毎に発生させる第２の乱数発生ステップと、
前記第２の乱数発生ステップの処理により発生された前記第３の鍵を、前記第２の鍵で暗号化する第２の暗号化ステップと、
前記第２の暗号化ステップの処理により暗号化された前記第３の鍵を前記記録媒体の記録単位に記録するように記録を制御する第２の記録制御ステップとをさらに含むことを特徴とする請求項８に記載の情報記録方法。
【請求項１０】　前記第２の鍵は、前記記録媒体毎に固有の値とされるとともに、前記秘密鍵の世代が変わる毎に、前記第１の乱数発生ステップの処理により新規に生成されることを特徴とする請求項８に記載の情報記録方法。
【請求項１１】　前記記憶制御ステップの処理では、１世代の前記秘密鍵を記憶するように記憶を制御し、演算により他の世代の前記秘密鍵を生成することを特徴とする請求項７に記載の情報記録方法。
【請求項１２】　前記第１の鍵の世代番号は、前記生成ステップの処理で用いた前記秘密鍵の世代に対応することを特徴とする請求項７に記載の情報記録方法。
【請求項１３】　着脱可能な記録媒体にデータを記録する情報記録装置用のプログラムであって、
少なくとも１以上の世代の秘密鍵を記憶するように記憶を制御する記憶制御ステップと、
前記記録媒体の媒体識別情報と前記秘密鍵から第１の鍵を生成する生成ステップと、
前記記録媒体に記録するデータを暗号化するために用いる第２の鍵を前記第１の鍵で暗号化する暗号化ステップと、
前記暗号化ステップの処理により暗号化された前記第２の鍵を、前記第１の鍵の世代番号とともに前記記録媒体に記録するように記録を制御する記録制御ステップとを

含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項１４】　着脱可能な記録媒体に記録されているデータを再生する情報再生装置において、
少なくとも１以上の世代の秘密鍵を記憶する記憶手段と、
前記記録媒体から、第１の鍵で暗号化された第２の鍵、前記第２の鍵を暗号化した前記第１の鍵の世代番号、および前記記録媒体の媒体識別情報を読み出す第１の読み出し手段と、
前記第１の読み出し手段により読み出された前記媒体識別情報および前記世代番号に対応する前記秘密鍵から前記第１の鍵を生成する生成手段と、
前記生成手段により生成された前記第１の鍵で、前記第２の鍵を復号する第１の復号手段とを備えることを特徴とする情報再生装置。

【請求項１５】　前記記録媒体は、複数の記録単位に分割されており、
前記記録単位に記録されている前記第２の鍵で暗合化された第３の鍵を読み出す第２の読み出し手段と、
前記第１の復号手段により復号された前記第２の鍵で、前記第２の読み出し手段により読み出された前記第３の鍵を復号する第２の復号手段と、
前記第２の復号手段により復号された前記第３の鍵で、前記データを復号する第３の復号手段とをさらに備えることを特徴とする請求項１４に記載の情報再生装置。

【請求項１６】　前記記憶手段は、１世代の前記秘密鍵を記憶し、演算により他の世代の前記秘密鍵を生成することを特徴とする請求項１４に記載の情報再生装置。

【請求項１７】　前記第１の鍵の世代番号は、前記生成手段で用いた前記秘密鍵の世代に対応することを特徴とする請求項１４に記載の情報再生装置。

【請求項１８】　着脱可能な記録媒体に記録されているデータを再生する情報再生装置の情報再生方法において、
少なくとも１以上の世代の秘密鍵を記憶するように記憶を制御する記憶制御ステップと、
前記記録媒体から、第１の鍵で暗号化された第２の鍵、前記第２の鍵を暗号化した前記第１の鍵の世代番号、および前記記録媒体の媒体識別情報を読み出す第１の読み出しステップと、
前記第１の読み出しステップの処理により読み出された前記媒体識別情報および前記世代番号に対応する前記秘密鍵から前記第１の鍵を生成する生成ステップと、
前記生成ステップの処理により生成された前記第１の鍵で、前記第２の鍵を復号する第１の復号ステップとを含むことを特徴とする情報再生方法。

【請求項１９】　前記記録媒体は、複数の記録単位に分割されており、
前記記録単位に記録されている前記第２の鍵で暗合化された第３の鍵を読み出す第２の読み出しステップと、
前記第１の復号ステップの処理により復号された前記第２の鍵で、前記第２の読み出しステップの処理により読み出された前記第３の鍵を復号する第２の復号ステップと、
前記第２の復号ステップの処理により復号された前記第３の鍵で、前記データを復号する第３の復号ステップとをさらに含むことを特徴とする請求項１８に記載の情報再生方法。

【請求項２０】　前記記憶制御ステップの処理では、１世代の前記秘密鍵を記憶し、演算により他の世代の前記秘密鍵を生成することを特徴とする請求項１８に記載の情報再生方法。

【請求項２１】　前記第１の鍵の世代番号は、前記生成ステップの処理で用いた前記秘密鍵の世代に対応することを特徴とする請求項１８に記載の情報再生方法。

【請求項２２】　着脱可能な記録媒体に記録されているデータを再生する情報再生装置用のプログラムであって、
少なくとも１以上の世代の秘密鍵を記憶するように記憶を制御する記憶制御ステップと、
前記記録媒体から、第１の鍵で暗号化された第２の鍵、前記第２の鍵を暗号化した前記第１の鍵の世代番号、および前記記録媒体の媒体識別情報を読み出す読み出しステップと、
前記読み出しステップの処理により読み出された前記媒体識別情報および前記世代番号に対応する前記秘密鍵から前記第１の鍵を生成する生成ステップと、
前記生成ステップの処理により生成された前記第１の鍵で、前記第２の鍵を復号する復号ステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項２３】　情報記録装置または情報再生装置によりデータが記録または再生される記録媒体において、
前記記録媒体に固有の値である媒体識別情報と、
前記媒体識別情報と前記情報記録装置からの秘密鍵により生成される第１の鍵で暗号化された、前記データを暗号化するために用いる前記第２の鍵とが記録されているとともに、
前記第１の鍵で暗号化されている前記第２の鍵は、前記第１の鍵の世代番号と関連付けられて記録されていることを特徴とする記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、情報記録装置および方法、情報再生装置および方法、並びに記録媒体に関し、特に、著作権を有するコンテンツが不正に利用されることなく、安全に暗号化されたコンテンツを記録媒体に記録または再生できるようにした情報記録装置および方法、情報再生装置および方法、並びに記録媒体に関す

る。

【０００２】

【従来の技術】近年、情報をデジタル的に記録する記録機器および記録媒体が普及しつつある。これらの記録機器および記録媒体は、例えば、映像や音楽のデータを劣化させることなく記録し、再生するので、データを、その質を維持しながら何度もコピーすることができる。しかしながら、映像や音楽の著作権者にしてみれば、自らが著作権を有する映像や音楽のデータが、その質を維持しながら何度も不正にコピーされ、市場に流通してしまう恐れがある。このため、記録機器および記録媒体の側で、著作権を有するデータが不正にコピーされるのを防ぐ要請がある。

【０００３】例えば、ミニディスク（MD）（商標）システムにおいては、SCMS(Serial CopyManagement System)と呼ばれる方法が用いられている。これは、デジタルインタフェースによって、音楽データとともに伝送される情報により、音楽データが、copy free（コピー自由）、copy once allowed（コピー１回可）、またはcopyprohibited（コピー禁止）のうちのいずれのデータであるのかを表す。ミニディスクレコーダは、デジタルインタフェースから音楽データを受信した場合、SCMSを検出し、これが、copy prohibitedであれば、音楽データをミニディスクに記録せず、copy once allowedであれば、これをcopy prohibitedに変更し、受信した音楽データとともに記録し、copy freeであれば、これをそのまま、受信した音楽データとともに記録する。

【０００４】このようにして、ミニディスクシステムにおいては、SCMSを用いて、著作権を有するデータが不正にコピーされるのが防止されている。

【０００５】また、著作権を有するデータが不正にコピーされるのを防ぐ別の例としては、Digital Versatile Disk(DVD)（商標）システムにおける、コンテンツスクランブルシステムがあげられる。このシステムでは、ディスク上の、著作権を有するデータが全て暗号化され、ライセンスを受けた記録機器だけが暗号鍵を与えられ、これにより暗号化されているデータを復号し、意味のあるデータを得ることができるようになされている。そして、記録機器は、ライセンスを受ける際に、不正コピーを行わない等の動作規定に従うように設計される。このようにして、DVDシステムにおいては、著作権を有するデータが不正にコピーされることが防止されている。

【０００６】しかしながら、ミニディスクシステムが採用している方式では、SCMSがcopy once allowedであれば、これをcopy prohibitedに変更し、受信したデータとともに記録するなどの動作規定に従わない記録機器が、不正に製造されると、それによるコピーを防止することができない。

【０００７】また、DVDシステムが採用している方式は、ROM（Read Only Memory）メディアに対しては有効であるが、ユーザがデータを記録可能なRAM（Random Access Memory）メディアにおいては有効ではない。RAMメディアにおいては、不正者は、暗号を解読できない場合であっても、ディスク上のデータを全部、新しいディスクに不正にコピーすることによって、ライセンスを受けた正当な記録機器で動作するディスクを新たに作ることができるからである。

【０００８】そこで、本出願人は、先に提出した特願平１０－２５３１０において、個々の記録媒体を識別する為の情報（以下、媒体識別情報と記述する）を、他のデータとともに記録媒体に記録し、ライセンスを受けた機器でしか、その記録媒体の媒体識別情報にアクセスできないようにする方法を提案した。その方法では、記録媒体上のデータは、媒体識別情報とライセンスを受けることにより得られる秘密キー（マスタキー）により暗号化され、ライセンスを受けていない機器がその暗号化されたデータを読み出したとしても、そのデータは意味をなさないようにしている。各機器はライセンスを受ける際、不正な複製ができないようにその動作が規定されている。

【０００９】ライセンスを受けていない機器は媒体識別情報にアクセスできず、また、媒体識別情報は個々の媒体毎に個別の値となっているため、ライセンスを受けていない機器がアクセス可能な全ての情報（暗号化されている）を新たな媒体に複製したとしても、そのようにして作成された媒体の情報は、ライセンスを受けていない機器は勿論、ライセンスを受けた機器においても、正しく読み出す事ができない。このようにして、不正な複製が行われる事が防止されている。

【００１０】

【発明が解決しようとする課題】先の提案におけるライセンスにより得られる秘密キーは、全機器において共通である必要があった。これは、１つの機器で記録された媒体が、他の機器で再生可能である（インターオペラビリティを確保する）為に必要な条件であった。

【００１１】この為に、１つの機器が攻撃者により攻撃を受け、その機器が保持していた秘密キーが暴かれてしまった場合、全ての機器の秘密キーが暴かれてしまったのと同じ事になり、すなわち、秘密キーが暴かれる前に記録されたデータは勿論、秘密キーが暴かれた後に記録されたデータも、その暴かれた秘密キーを用いて、解読されてしまうといった課題があった。

【００１２】そのようなことを防ぐために、秘密キーが暴かれたことがわかったときや、定期的に、機器に記憶されている秘密キーを更新することが考えられる。更新された秘密キーが用いられることにより、その秘密キーで暗号化されたデータは、暴かれた秘密キーでは解読されないことになる。

【００１３】しかしながら、上述したように、機器に記憶されている秘密キーを更新した場合、古い秘密キーを

用いて暗号化されたデータが復号できなくなるといった課題があった。

【００１４】本発明はこのような状況に鑑みてなされたものであり、秘密キーを古い世代のキーも含めて複数記憶するか、または、最新世代の秘密キーから古い世代の秘密キーを作成できるようにすることにより、機器に記憶されている秘密キーを更新した場合でも、古い世代の秘密キーを利用して暗号化されたデータを復号できるようにするものである。

【００１５】

【課題を解決するための手段】請求項１に記載の情報記録装置は、少なくとも１以上の世代の秘密鍵を記憶する記憶手段と、記録媒体の媒体識別情報と秘密鍵から第１の鍵を生成する生成手段と、記録媒体に記録するデータを暗号化するために用いる第２の鍵を第１の鍵で暗号化する第１の暗号化手段と、第１の暗号化手段により暗号化された第２の鍵を、第１の鍵の世代番号とともに記録媒体に記録する第１の記録手段とを備えることを特徴とする。

【００１６】請求項７に記載の情報記録方法は、少なくとも１以上の世代の秘密鍵を記憶するように記憶を制御する記憶制御ステップと、記録媒体の媒体識別情報と秘密鍵から第１の鍵を生成する生成ステップと、記録媒体に記録するデータを暗号化するために用いる第２の鍵を第１の鍵で暗号化する第１の暗号化ステップと、第１の暗号化ステップの処理により暗号化された第２の鍵を、第１の鍵の世代番号とともに記録媒体に記録するように記録を制御する第１の記録制御ステップとを含むことを特徴とする。

【００１７】請求項１３に記載の記録媒体のプログラムは、少なくとも１以上の世代の秘密鍵を記憶するように記憶を制御する記憶制御ステップと、記録媒体の媒体識別情報と秘密鍵から第１の鍵を生成する生成ステップと、記録媒体に記録するデータを暗号化するために用いる第２の鍵を第１の鍵で暗号化する暗号化ステップと、暗号化ステップの処理により暗号化された第２の鍵を、第１の鍵の世代番号とともに記録媒体に記録するように記録を制御する記録制御ステップとを含むことを特徴とする。

【００１８】請求項１４に記載の情報再生装置は、少なくとも１以上の世代の秘密鍵を記憶する記憶手段と、記録媒体から、第１の鍵で暗号化された第２の鍵、第２の鍵を暗号化した第１の鍵の世代番号、および記録媒体の媒体識別情報を読み出す第１の読み出し手段と、第１の読み出し手段により読み出された媒体識別情報および世代番号に対応する秘密鍵から第１の鍵を生成する生成手段と、生成手段により生成された第１の鍵で、第２の鍵を復号する第１の復号手段とを備えることを特徴とする。

【００１９】請求項１８に記載の情報再生方法は、少なくとも１以上の世代の秘密鍵を記憶するように記憶を制御する記憶制御ステップと、記録媒体から、第１の鍵で暗号化された第２の鍵、第２の鍵を暗号化した第１の鍵の世代番号、および記録媒体の媒体識別情報を読み出す第１の読み出しステップと、第１の読み出しステップの処理により読み出された媒体識別情報および世代番号に対応する秘密鍵から第１の鍵を生成する生成ステップと、生成ステップの処理により生成された第１の鍵で、第２の鍵を復号する第１の復号ステップとを含むことを特徴とする。

【００２０】請求項２２に記載の記録媒体のプログラムは、少なくとも１以上の世代の秘密鍵を記憶するように記憶を制御する記憶制御ステップと、記録媒体から、第１の鍵で暗号化された第２の鍵、第２の鍵を暗号化した第１の鍵の世代番号、および記録媒体の媒体識別情報を読み出す読み出しステップと、読み出しステップの処理により読み出された媒体識別情報および世代番号に対応する秘密鍵から第１の鍵を生成する生成ステップと、生成ステップの処理により生成された第１の鍵で、第２の鍵を復号する復号ステップとを含むことを特徴とする。

【００２１】請求項２３に記載の記録媒体は、記録媒体に固有の値である媒体識別情報と、媒体識別情報と情報記録装置からの秘密鍵により生成される第１の鍵で暗号化された、データを暗号化するために用いる第２の鍵とが記録されているとともに、第１の鍵で暗号化されている第２の鍵は、第１の鍵の世代番号と関連付けられて記録されていることを特徴とする。

【００２２】請求項１に記載の情報記録装置、請求項７に記載の情報記録方法、および請求項１３に記載の記録媒体のプログラムにおいては、少なくとも１以上の世代の秘密鍵が記憶され、記録媒体の媒体識別情報と秘密鍵から第１の鍵が生成され、記録媒体に記録するデータを暗号化するために用いる第２の鍵が第１の鍵で暗号化され、暗号化された第２の鍵が第１の鍵の世代番号とともに記録媒体に記録される。

【００２３】請求項１４に記載の情報再生装置、請求項１８に記載の情報再生方法、および請求項２２に記載の記録媒体のプログラムにおいては、少なくとも１以上の世代の秘密鍵が記憶され、記録媒体から、第１の鍵で暗号化された第２の鍵、第２の鍵を暗号化した第１の鍵の世代番号、および記録媒体の媒体識別情報が読み出され、読み出された媒体識別情報および世代番号に対応する秘密鍵から第１の鍵が生成され、生成された第１の鍵で、第２の鍵が復号される。

【００２４】請求項２３に記載の記録媒体においては、記録媒体に固有の値である媒体識別情報と、媒体識別情報と情報記録装置からの秘密鍵により生成される第１の鍵で暗号化された、データを暗号化するために用いる第２の鍵とが記録されているとともに、第１の鍵で暗号化されている第２の鍵は、第１の鍵の世代番号と関連付け

られて記録されている。

【００２５】

【発明の実施の形態】以下に本発明の実施の形態を説明する。図１は、本発明を適用した光ディスク記録再生装置の構成例を表している。入力部１は、ボタン、スイッチ、リモートコントローラなどにより構成され、ユーザにより入力操作されたとき、その入力操作に対応する信号を出力する。例えば、マイクロコンピュータなどにより構成される制御回路２は、記憶されている所定のコンピュータプログラムに従って、装置全体を制御する。

【００２６】記録再生回路３は、暗号化部４と復号部５を有し、復号部５は、ピックアップ６により、光ディスク７から再生されたデータを復号し、再生信号として外部に出力する。暗号化部４は、外部から記録信号の供給を受け取ると、これを暗号化し、ピックアップ６に供給して、光ディスク７に記録させる。

【００２７】ピックアップ６は、レーザビームを光ディスク７に照射することで、データの記録再生を行う。スピンドルモータ９は、サーボ回路８によって制御され、光ディスク７を回転させる。サーボ回路８は、スピンドルモータ９を駆動することにより、光ディスク７を所定の速度で（例えば線速度一定で）回転させる。サーボ回路８はまた、ピックアップ６のトラッキングおよびフォーカシングの他、スレッドサーボを制御する。乱数発生回路１０は、制御回路２の制御により、所定の乱数を発生する。

【００２８】光ディスク７には、図２に示すような構造を有するデータが記録されている。光ディスク７のリードインエリアには、光ディスク７のID（以下、DiscIDと称する）を、予め定められたM系列符号で暗号化したEDiscID、世代番号と関連づけられたディスクキーKdをイフェクティブマスタキーKemで暗号化した暗号化ディスクキーEKdが記録されている。図２に示した例では、世代番号１と世代番号３の暗号化ディスクキーEKdが記録されている。

【００２９】DiscIDとは、光ディスク７を識別するための異なる固有の値である。また、ディスクキーKdは、光ディスク７毎に固有の値であるとともに、記録再生回路３のマスタキーKmの世代番号毎にも異なる固有の値である。すなわち、マスタキーKmの世代が更新される毎に、それぞれの世代に対応するディスクキーKdj（j=1,2,3…）が存在する（ここでKdjのｊは、世代番号を示すが、特に区別する必要がない場合は、Kdとも記述する）。

【００３０】M系列符号は、所定の周期で、″０″と″１″の２値がランダムに出現する疑似ランダム２値信号（一種の疑似乱数）であり、DiscIDは、例えば、ファイル名やデイレクトリ情報などのTOC(Table Of Contents)データ内に、予め設定された所定のM系列符号に基づいて埋め込むことで暗号化されている。すなわち、DiscIDは、TOCデータのエッジの時間ずれとして記録される。このような暗号化を行うと、TOCデータはM系列符号がなくとも読み取ることができるが（TOCデータは暗号化されないが）、DiscIDはM系列符号がないと読み取る（復号する）ことができなくなる。このようなM系列符号に基づく暗号化に関する技術は、特願平09-288960号として本出願人が先に提案している。なお、この所定のM系列符号は、著作権者から適正なライセンスを受ける際、後述するマスタキーKmとともに、ライセンスを受けた者に与えられる。

【００３１】イフェクティブマスタキーKemは、以下に示す式（１）に従い、マスタキーKmとDiscIDの結合にhash関数を適用して計算される。

【００３２】

イフェクティブマスタキーKem＝hash（マスタキーKm＋DiscID）・・・（１）

ここでマスタキーKmは、著作権者等から適正にライセンスを受けた者（光ディスク記録再生装置）にだけ与えられる秘密のキーである。また、ここで、例えば、ＡとＢの結合とは、それぞれが３２ビットであるとき、Ａの後方にＢを結合して、６４ビットのデータとすることを意味する。

【００３３】光ディスク７のデータエリアの各セクタSi(i=1,2,...)は、ヘッダおよびメインデータ部で構成され、ヘッダには、セクタキーKsiをディスクキーKdで暗号化した暗号化セクタキーEKsi(i=1,2,...)が格納されている（ここでKsiのiは、セクタの番号を示し、セクタキーはセクタ毎に異なるのでKsiと記述するが、特に区別する必要がない場合は、Ksとも記述する）。

【００３４】また、光ディスク７には、複数の世代のディスクキーKd（イフェクティブマスタキーKemにより暗号化されている）が記録されているので、どの世代のディスクキーが用いられて暗号化されたのかを識別できるように、データエリアの各セクタのヘッダには、用いられたディスクキーKdの世代番号も記録されている。図２に示した例では、光ディスク７に記録されているディスクキーKdの世代は、世代番号１と世代番号３であるので、その世代番号１と世代番号３のディスクキーKdのみが用いられてセクタキーEKsは暗号化されている。

【００３５】メインデータ部には、コンテンツデータをセクタキーKsiで暗号化した暗号化コンテンツデータが格納されている。

【００３６】図３は、暗号化部４の構成例を表している。DiscID暗号化復号回路２１は、光ディスク７から読み出された暗号化ディスクID、すなわちEDiscIDを、M系列符号発生回路２２から供給されるM系列符号に基づいて復号し、DiscIDを生成する。DiscID暗号化復号回路２１はまた、乱数発生回路１０から発生された乱数をDiscIDとして受け取り、M系列符号発生回路２２から供給されるM系列符号に基づいて、上述したように、入力さ

れるTOC情報に埋め込むように暗号化して、EDiscIDを生成し、光ディスク７に記録する。

【００３７】M系列符号発生回路２２は、例えば、直列接続された複数のフリップフロップとExclusive-OR（イクスクルーシブオア）回路から構成したり、あるいは、ROM、EEPROMなどで構成することもできる。

【００３８】Kem発生モジュール２３のKmメモリ２４は、複数のマスタキーKmを記憶する。Kem発生モジュール２３のhash関数回路２５は、マスタキーKmとDiscIDの結合を生成し、これにhash関数を適用してイフェクティブマスタキーKemを算出する。

【００３９】Kd暗号化復号回路２６は、光ディスク７から読み出された暗号化ディスクキーEKdを、イフェクティブマスタキーKemで復号して、ディスクキーKdを生成する。Kd暗号化復号回路２６はまた、乱数発生回路１０から発生された乱数をディスクキーKdとして受け取り、イフェクティブマスタキーKemで暗号化して暗号化ディスクキーEKdを生成し、光ディスク７に記録する。

【００４０】Ks暗号化回路２７は、乱数発生回路１０から発生された乱数をセクタキーKsとして受け取り、ディスクキーKdで暗号化して暗号化セクタキーEKsを生成し、光ディスク７に記録する。コンテンツデータ暗号化回路２８は、セクタキーKsで、コンテンツデータを暗号化し、光ディスク７に記録する。

【００４１】なお、図３の例では、暗号化回路として、Ks暗号化回路２７とコンテンツデータ暗号化回路２８を、それぞれ別々の構成として記載したが、これらは、勿論、一つの暗号化回路として構成してもよい（復号回路も同様である）。

【００４２】次に、図４に、復号部５の構成例を示す。EDiscID復号回路４１は、光ディスク７から読み出されたEDiscIDを、M系列符号発生回路４２から供給されるM系列符号に基づいて復号して、DiscIDを生成する。M系列符号発生回路４２は、M系列符号発生回路２２と同様の構成を有し、M系列符号発生回路２２と同一のM系列符号を発生するようになされている。

【００４３】Kem発生モジュール４３のKmメモリ４４は、複数のマスタキーKmを記憶する。Kem発生モジュール４３のhash関数回路４５は、マスタキーKmとDiscIDの結合を生成し、これにhash関数を適用してイフェクティブマスタキーKemを計算する。このKem発生モジュール４３は、Kem発生モジュール２３と同一の構成とされ、両者を兼用するようにしてもよい。ここで、Kmメモリ２４とKmメモリ４４に記憶されるマスタキーについて、図５を参照して説明する。

【００４４】Kmメモリ２４，４４には、マスターキーKmが、世代が若い順に複数記憶される。図５は、世代番号１乃至３のマスタキーKmが記憶されている例を示している。新たな世代のマスタキーKmは、例えば、その新たな世代のマスタキーKmが記録された光ディスク７を介して配布されたり、インターネットなどのネットワークを介して配布される。マスタキーKmを記憶する各デバイス（光ディスク記録再生装置）毎に、そのデバイス固有の暗号鍵を保持させ、Kmメモリ２４，４４に記憶されるマスタキーKmを、その暗号鍵で暗号化してから記憶させるようにしても良い。

【００４５】EKd復号回路４６は、光ディスク７から読み出された暗号化ディスクキーEKdを、イフェクティブマスタキーKemで復号して、ディスクキーKdを算出する。EKs復号回路４７は、光ディスク７から各セクタSiのヘッダに記録されている暗号化セクタキーEKsを読み出し、ディスクキーKdで復号して、セクタキーKsを算出する。コンテンツデータ復号回路４８は、光ディスク７から読み出された暗号化されているコンテンツデータを、セクタキーKsで復号する。

【００４６】世代判別回路４９は、データエリアのヘッダを読み出し、メインデータ部に記録されているコンテンツデータが、どの世代のセクタキーKsを用いて暗号化されているかを判断し、その判断結果をKmメモリ４４に出力する。Kmメモリ４４は、世代判別回路４９から出力された世代に関するデータに従って、記憶されているマスタキーKmをhash関数回路４５に出力する。

【００４７】次に、コンテンツデータが光ディスク７に記録される場合の暗号化部４における処理手順を、図６のフローチャートを参照して説明する。ステップＳ１において、DiscID暗号化復号回路２１は、光ディスク７のリードインエリアに、EDiscIDが書き込まれているか否かの判定を行い、Kd暗号化復号回路２６は、光ディスク７のリードインエリアに、暗号化ディスクキーEKdが書き込まれているか否かの判定を行う。EDiscIDと暗号化ディスクキーEKdが共に書き込まれていないと判定された場合、ステップＳ２に進み、乱数発生回路１０は、１２８ビットの乱数を発生し、DiscIDとして、DiscID暗号化復号回路２１に出力する。

【００４８】ステップＳ３において、DiscID暗号化復号回路２１は、乱数発生回路１０から供給されたDiscIDを、M系列符号発生回路２２から供給されたM系列符号に基づいて、上述したように、TOC情報中に埋め込むようにして暗号化して、EDiscIDを生成し、光ディスク７のリードインエリアに記録する。M系列符号回路２２が供給するM系列符号は、著作権者から適正なライセンスを受けるときに与えられたものである。

【００４９】次に、ステップＳ４において、Kem発生モジュール２３のhash関数回路２５は、Kem発生モジュール２３のKmメモリ２４から、最新世代のマスタキーKmを読み出す。Kem発生モジュール２３のhash関数回路２５は、ステップＳ５で、上述した式（１）に従い、光ディスク７のDiscID、およびKmメモリ２４から読み出したマスタキーKmの結合にhash関数を適用して、イフェクティブマスタキーKemを計算し、Kd暗号化復号回路２６に供

給する。

【００５０】次に、ステップＳ６において、乱数発生回路１０は、４０ビットの乱数を発生し、ディスクキーKdとして、Kd暗号化復号回路２６に出力する。Kd暗号化復号回路２６は、ステップＳ７において、乱数発生回路１０から供給されたディスクキーKdを、hash関数回路２５から受け取ったイフェクティブマスタキーKemにより暗号化して、暗号化ディスクキーEKdを生成し、光ディスク７のリードインエリアに記録する。

【００５１】一方、ステップＳ１で、光ディスク７にEDiscIDと暗号化ディスクキーEKdが書き込まれていると判定された場合、ステップＳ８に進み、DiscID暗号化復号回路２１は、この光ディスク７から読み出されたEDiscIDを、M系列符号発生回路２２から供給されたM系列符号で復号して、DiscIDを得る。

【００５２】ステップＳ９において、Kem発生モジュール２３のhash関数回路２５は、Kem発生モジュール２３のKmメモリ２４から、最新世代のマスタキーKmを読み出す。Kem発生モジュール２３のhash関数回路２５は、ステップＳ１０で、上述した式（１）に従い、光ディスク７のDiscIDとマスタキーKmの結合にhash関数を適用して、イフェクティブマスタキーKemを計算し、Kd暗号化復号回路２６に供給する。

【００５３】次に、ステップＳ１１において、Kd暗号化復号回路２６は、光ディスク７から読み出された暗号化ディスクキーEKdを、hash関数回路２５から受け取ったイフェクティブマスタキーKemで復号して、ディスクキーKdを得る。Kd暗号化復号回路２６は、ディスクキーKdを、Ks暗号化回路２７に出力する。

【００５４】ステップＳ７またはＳ１１の処理の後、乱数発生回路１０は、ステップＳ１２において、４０ビットの乱数を発生し、セクタキーKsとして、Ks暗号化回路２７、およびコンテンツデータ暗号化回路２８に出力する。Ks暗号化回路２７は、ステップＳ１３において、Kd暗号化復号回路２６（暗号化ディスクキーEKdが光ディスク７に記録されている場合）、または乱数発生回路１０（暗号化ディスクキーEKdが光ディスク７に記録されていない場合）から受け取ったディスクキーKdで、乱数発生回路１０から受け取ったセクタキーKsを暗号化して、暗号化セクタキーEKsを生成する。Ks暗号化回路２７はまた、その暗号化セクタキーEKsを、光ディスク７のデータエリアのヘッダに記録する。

【００５５】次に、ステップＳ１４において、コンテンツデータ暗号化回路２８は、セクタキーKsにより、コンテンツデータを暗号化し、光ディスク７のデータエリアのメインデータ部に記録する。

【００５６】ステップＳ１５において、暗号化部４の各回路は、全てのコンテンツデータを記録したか否かの判定を行う。全てのコンテンツデータがまだ記録されていないと判定された場合、ステップＳ１６に進み、暗号化部４の各回路は、光ディスク７の、まだデータを記録していないセクタにアクセスし、ステップＳ１２に戻り、以下同様の処理を繰り返す。一方、ステップＳ１５で、全てのコンテンツデータが記録されたと判定された場合、暗号化部４の各回路は、全ての記録処理を終了する。

【００５７】以上のようにして、著作権者から適正なライセンスを受けるときに、与えられた所定のM系列符で、暗号化されたDiscIDを復号し、DiscIDを得ることにより、暗号化した情報が記録媒体に記録される。これにより、例えば、著作権者から適正にライセンスを受けていない者が、このディスクのコンテンツデータを既存の記録媒体（DiscIDが記録されていない記録媒体）に複製したとしても、そのコンテンツデータを、意味のある情報として再生することができない。

【００５８】次に、図７のフローチャートを参照して、復号部５により行われる、コンテンツデータの再生処理を説明する。ステップＳ２１において、EDiscID復号回路４１は、光ディスク７のリードインエリアから読み出された、暗号化されたDiscIDであるEDiscIDを受け取る。また、世代判別回路４９は、光ディスク７のデータエリアのヘッダを受け取る。

【００５９】EDiscID復号回路４１は、ステップＳ２２において、M系列符号発生回路４２から供給されたM系列符号に基づいて、EDiscIDを復号してDiscIDを得た後、Kem発生モジュール４３のhash関数回路４５に出力する。

【００６０】次に、ステップＳ２３において、Kem発生モジュール４３のhash関数回路４５は、EDiscID復号回路４１から出力されたDiscIDを受け取るとともに、世代判別回路４９が判別した世代に従って、Kmメモリ４４から読み出されたマスタキーKmを受け取り、上述した式（１）に従い、光ディスク７のDiscIDとマスタキーKmの結合にhash関数を適用してイフェクティブマスタキーKemを算出し、EKd復号回路４６に供給する。

【００６１】ステップＳ２４において、EKd復号回路４６は、光ディスク７のリードインエリアから読み出された暗号化ディスクキーEKdを受け取る。EKd復号回路４６は、ステップＳ２５で、この読み出された暗号化ディスクキーEKdを、hash関数回路４５から受け取ったイフェクティブマスタキーKemで復号して、ディスクキーKdを算出し、EKs復号回路４７に出力する。

【００６２】次に、ステップＳ２６において、EKs復号回路４７は、光ディスク７のデータエリアから読み出された各セクタの暗号化セクタキーEKsi（i=1,2,...）を受け取る。EKs復号回路４７は、ステップＳ２７で、この読み出された暗号化セクタキーEKsiを、EKd復号回路４６から受け取ったディスクキーKdで復号して、セクタキーKsiを算出し、コンテンツデータ復号回路４８に出力する。

【００６３】ステップＳ２８において、コンテンツデータ復号回路４８は、光ディスク７から読み出された暗号化されているコンテンツデータを受け取る。コンテンツデータ復号回路４８は、ステップＳ２９で、この読み出された暗号化されているコンテンツデータを、EKs復号回路４７から受け取ったセクタキーKsiで復号し、再生信号として出力する。

【００６４】次に、ステップＳ３０において、復号部５の各回路は、光ディスク７のデータエリアから、全てのコンテンツデータを読み出したか否かの判定を行う。全てのコンテンツデータがまだ読み出されていないと判定された場合、ステップＳ３１に進み、復号部５の各回路は、光ディスク７の、まだ読み出されていない次のセクタのデータの供給を受け、ステップＳ２６以降の処理を繰り返す。全てのコンテンツデータが読み出されたと判定された場合、復号部５の各回路は、全ての再生処理を終了する。

【００６５】このように、記録媒体のIDを生成し、所定のＭ系列符号で暗号化して、記録媒体に記録することで、著作権者から適正にライセンスを受けた者だけが、その記録媒体にアクセスできる。また、複数のマスタキーKmを記憶することにより、古い世代のマスタキーKmで暗号化されたデータでも復号（再生）することができる。

【００６６】なお、上述した実施の形態においては、Kmメモリ２４，４４が、世代毎のマスタキーKmを記憶するようにしたが、最新世代のマスタキーKmから過去の世代のマスタキーKmを生成するようにしても良い。すなわち、各デバイスに１方向性関数ｆを記憶させ、その１方向性関数ｆに最新世代のマスタキーKmを代入することにより、その１世代前のマスタキーKmを作成する。さらに古いマスタキーKmが必要な場合には、順次１方向性関数ｆに繰り返しマスタキーKmを代入することより、１世代づつ前の世代のマスタキーKmを作成する。

【００６７】この１方向性関数ｆとしては、例えば、Hash関数やＭＤ５（Message Diget 5）を用いることが可能である。

【００６８】本発明は、光ディスク以外の記録媒体にデータを記録または再生する場合にも適用が可能である。

【００６９】上述した一連の処理は、ハードウェアにより実行させることもできるが、ソフトウェアにより実行させることもできる。一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、記録媒体からインストールされる。

【００７０】この記録媒体は、コンピュータとは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク（フロッピディスクを含む）、光ディスク（CD-ROM（Compact Disk-Read Only Memory），DVD（Digital Versatile Disk）を含む、光磁気ディスク（MD（Mini-Disk）を含む）、若しくは半導体メモリなどよりなるパッケージメディアにより構成されるだけでなく、コンピュータに予め組み込まれた状態でユーザに提供される、プログラムが記録されているROMや、ハードディスクなどで構成される。

【００７１】

【発明の効果】本発明に記載の情報記録装置および方法、情報再生装置および方法、並びに記録媒体のプログラム、並びに記録媒体によれば、所定の世代の秘密キーを記憶し、記録媒体に記録されているデータを暗号化した秘密キーの世代に対応する秘密キーを生成し、その生成された秘密キーを用いて、記録媒体に暗号化されて記録されているデータを復号するようにしたので、記録されている秘密キーを更新した場合でも、古い秘密キーで暗号化されたデータを復号することが可能となる。

【図面の簡単な説明】

【図１】本発明を適用した光ディスク記録再生装置の一実施の形態の構成を示すブロック図である。

【図２】光ディスクに記録されるデータを説明する図である。

【図３】図１の暗号化部４の内部の構成を示す図である。

【図４】図１の復号部５の内部の構成を示す図である。

【図５】Ｋｍメモリに記憶されるデータを説明する図である。

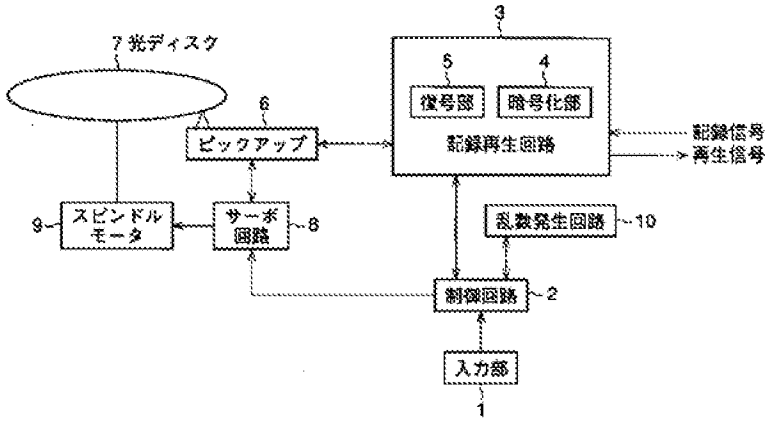
【図６】図１の暗号化部４の動作を説明するフローチャートである。

【図７】図１の復号部５の動作を説明するフローチャートである。

【符号の説明】

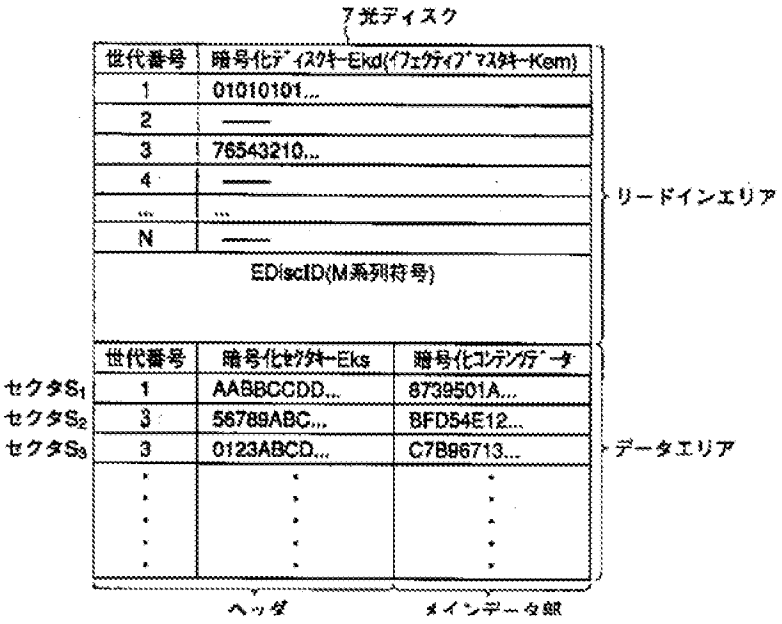
１　入力部，２　制御回路，３　記録再生回路，４　暗号化部，５　復号部，６　ピックアップ，７　光ディスク，８　サーボ回路，９　スピンドルモータ，１０　乱数発生回路，２１　DiscID暗号化復号回路，２２　Ｍ系列符号発生回路，２３　Kem発生モジュール，２４　Kmメモリ，２５　hash関数回路，２６　Kd暗号化復号回路，２７　Ks暗号化回路，２８　コンテンツデータ暗号化回路，４１　EDiscID復号回路，４２　Ｍ系列符号発生回路，４３　Kem発生モジュール，４４　Kmメモリ，４５　hash関数回路，４６　EKd復号回路，４７　EKs復号回路，４８　コンテンツデータ復号回路，　４９　世代判別回路

【図1】



光ディスク記録再生装置

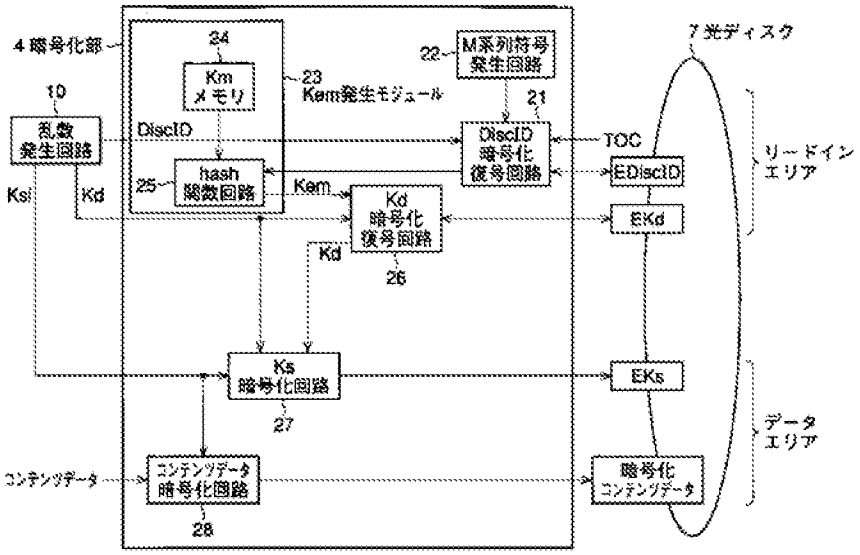
【図2】



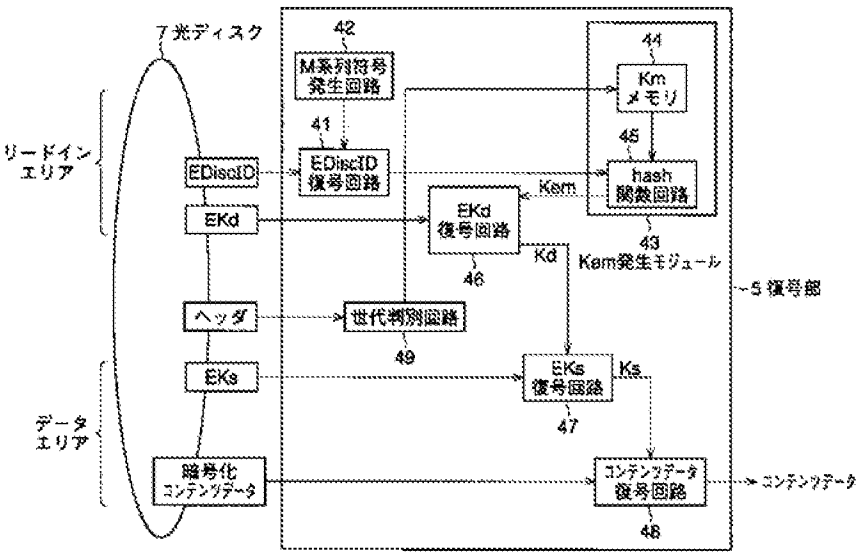
【図5】

世代番号	マスタキーKm
1	01234567...
2	FEDCBA98...
3	00112233...
4	——
...	...
N	——

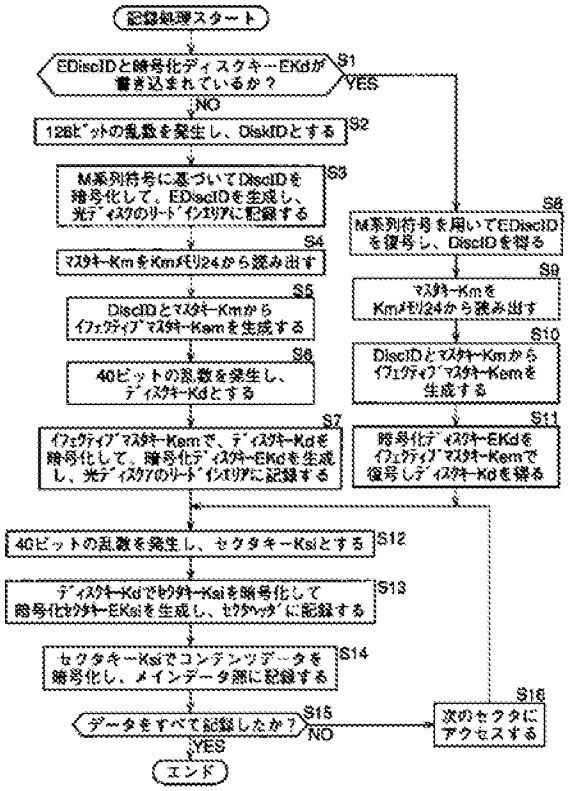
【図3】


4 暗号化部
24
Km メモリ
23 Kem発生モジュール
22 M系列符号発生回路
7 光ディスク
10
乱数発生回路
DiscID
21
DiscID 暗号化復号回路
TOC
リードインエリア
EDiscID
hash 関数回路
25
Kem
Ks
Kd
Kd 暗号化復号回路
EKd
Kd
26
Ks 暗号化回路
27
EKs
データエリア
コンテンツデータ
コンテンツデータ暗号化回路
28
暗号化コンテンツデータ

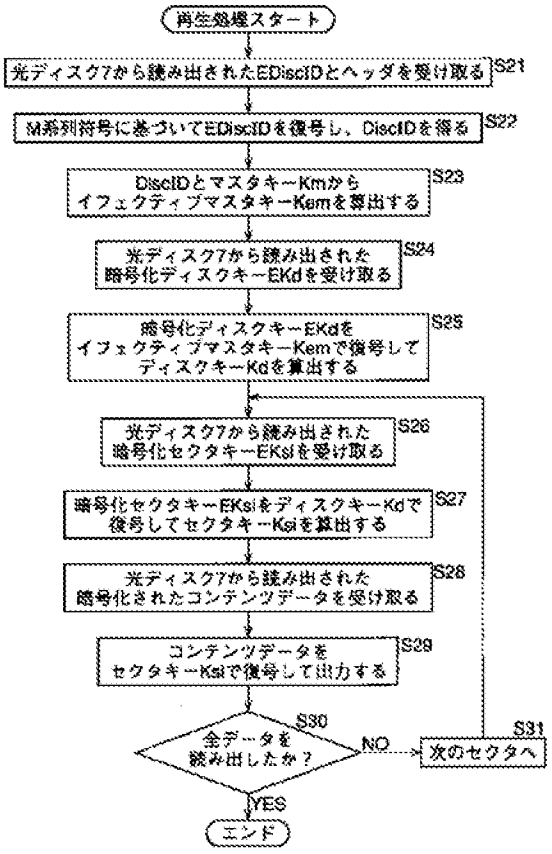
【図4】


7 光ディスク
42
M系列符号発生回路
44
Km メモリ
41
45
リードインエリア
EDiscID
EDiscID 復号回路
hash 関数回路
Kem
EKd
EKd 復号回路
Kd
43 Kem発生モジュール
46
5 復号部
ヘッダ
世代判別回路
49
EKs
EKs 復号回路
Ks
47
データエリア
暗号化コンテンツデータ
コンテンツデータ復号回路
コンテンツデータ
48

【図６】


記録処理スタート
EDiscIDと暗号化ディスクキーEKdが書き込まれているか？
S1
YES
NO
128ビットの乱数を発生し、DiskIDとする
S2
M系列符号に基づいてDiscIDを暗号化して、EDiscIDを生成し、光ディスクのリードインエリアに記録する
S3
マスターKmをKmメモリ24から読み出す
S4
DiscIDとマスターKmからイフェクティブマスターKemを生成する
S5
40ビットの乱数を発生し、ディスクキーKdとする
S6
イフェクティブマスターKemで、ディスクキーKdを暗号化して、暗号化ディスクキーEKdを生成し、光ディスクのリードインエリアに記録する
S7
M系列符号を用いてEDiscIDを復号し、DiscIDを得る
S8
マスターKmをKmメモリ24から読み出す
S9
DiscIDとマスターKmからイフェクティブマスターKemを生成する
S10
暗号化ディスクキーEKdをイフェクティブマスターKemで復号しディスクキーKdを得る
S11
40ビットの乱数を発生し、セクタキーKsiとする
S12
ディスクキーKdでセクタキーKsiを暗号化して暗号化セクタキーEKsiを生成し、セクタヘッダに記録する
S13
セクタキーKsiでコンテンツデータを暗号化し、メインデータ部に記録する
S14
データをすべて記録したか？
S15
NO
YES
次のセクタにアクセスする
S16
エンド

【図７】


再生処理スタート
光ディスク7から読み出されたEDiscIDとヘッダを受け取る
S21
M系列符号に基づいてEDiscIDを復号し、DiscIDを得る
S22
DiscIDとマスターKmからイフェクティブマスターKemを算出する
S23
光ディスク7から読み出された暗号化ディスクキーEKdを受け取る
S24
暗号化ディスクキーEKdをイフェクティブマスターKemで復号してディスクキーKdを算出する
S25
光ディスク7から読み出された暗号化セクタキーEKsiを受け取る
S26
暗号化セクタキーEKsiをディスクキーKdで復号してセクタキーKsiを算出する
S27
光ディスク7から読み出された暗号化されたコンテンツデータを受け取る
S28
コンテンツデータをセクタキーKsiで復号して出力する
S29
全データを読み出したか？
S30
NO
YES
次のセクタへ
S31
エンド